METHOD AND SYSTEM FOR SECURE TIME MANAGEMENT IN DIGITAL RIGHTS MANAGEMENT

BACKGROUND

[0001] The invention relates to electronic content security. More particularly, the invention relates to secure date and time management in the management of rights to electronic content.

[0002] More and more information is transmitted electronically in digital form. Virtually anything that can be represented by words, numbers, graphics, audio or video information, or a system of commands and instructions can be formatted into electronic digital information, also referred to as "digital content," or just "content." Electronic appliances of various types are all interconnected, providing their users with the potential to accomplish a myriad of tasks, such as telecommunications, financial transactions, business operations, research, and entertainment-related transactions.

[0003] A fundamental problem for digital content providers is extending their ability to control the use of proprietary information, such as copyrighted content. Content providers often want to limit the usage of the content to authorized activities and amounts. For example, commercial content providers are concerned with ensuring that they receive appropriate compensation for the use of content.

[0004] Content providers and distributors have employed a number of rights protection mechanisms to prevent unauthorized use of their content. Among these is Digital Rights Management (DRM). DRM relates to the licensing and control of the distribution and use of digital content. In general, DRM systems distribute digital content in an encrypted form. A set of rights is associated with the content, and only after acquiring

the rights to access a protected piece of digital content will a user be allowed to decrypt it.

[0005] DRM content distribution is becoming widespread as more devices, such as cellular telephones and personal digital assistants (PDAs) become DRM-enabled. According to conventional software architecture, as seen from a high-level system view, the software for the devices is one monolithic piece. For example, some current DRM solutions propose DRM function implementation within the software contained in the handheld device. More particularly, some conventional DRM solutions require the use of a dedicated "DRM player," such as a browser, media player, and the like.

[0006] An alternative approach is to divide the software into a platform part, having a platform software domain, which includes fundamental services and software components; and an application part, having an application software domain, which includes software components that are more closely related to specific device features. An example of such a system is described in U.S. Patent Application No. 10/413,044, "Method and System for Digital Rights Management," filed April 14, 2003. In the following, it is assumed that a software architecture having platform and application parts is used.

[0007] Currently there are competing DRM specifications, which include Open Mobile Alliance (OMA DRM), Windows Media Device (WM D-DRM), and several others.

[0008] The set of rights associated with an end user's use of a particular piece of content is often referred to as "usage rights". Some usage rights are date and time based. For example, the usage rights associated with a particular piece of content may stipulate that usage be allowed only between a specific start time (and date) and end time (and date). Alternatively, the usage rights associated may stipulate that usage be

allowed only for a certain amount of time, such as two hours, with the user selecting the start time and date. In general, usage rights that limit the use of the content using time as a parameter are referred to here as "time-based" usage rights. The term time-based is also used here in reference to the associated DRM content. These time-based usage rights must rely on a time reference to authorize and track the time-based usage rights.

[0009] The time reference, however, is not necessarily secure. A problem arises when an unscrupulous user gains access to the time reference and changes the time value so that access to the content is obtained outside the scope of the usage rights, i.e., for more time than was purchased. Not all current DRM specifications address adequately the susceptibility of content to unauthorized use through the manipulation of time reference values.

SUMMARY

[0010] It should be emphasized that the terms "comprises" and "comprising", when used in this description and claims, are taken to specify the presence of stated features, steps, or components, but the use of these terms does not preclude the presence or addition of one or more other features, steps, components, or groups thereof.

[0011] It should also be noted that the word "time" should be considered to be shorthand for "date and time" where the word "date" is not specifically mentioned.

[0012] In one aspect of the invention, a method is disclosed for establishing and maintaining secure date and time information about a user equipment (UE) in relation forwarding time-based Digital Rights Management-protected (DRM-protected) data to the UE. A secure time reference is retrieved from a secure time source. A secure time

offset representative of a time difference between the secure time reference and a UE time value associated with the UE is then determined. The secure date and time information for the UE is a combination of the secure time offset and the device time value.

[0013] In another aspect, the secure date and time information is maintained even when the UE time value is changed by an application. The secure time offset is updated when the UE time value is changed by an application to compensate for the change. In general, the term application refers to a piece of software that interfaces to users to provide services to the users by utilizing other resources inside and/or outside the UE.

[0014] In still another aspect of the invention, a system is disclosed for establishing and maintaining secure date and time information about a UE in relation to forwarding time-based DRM-protected data to the UE. The system includes logic that retrieves a secure time reference from a secure time source and logic that determines a secure time offset representative of a time difference between the secure time reference and a UE time value associated with the UE. The secure date and time information for the UE is a combination of the secure time offset and the device time value.

[0015] In yet another aspect, a UE includes logic that maintains the secure date and time information even when the UE time value is changed by an application. The secure time offset is updated when the UE time value is changed by an application to compensate for the change.

BRIEF DESCRIPTION OF THE DRAWINGS

[0016] Objects and advantages of the present invention will become apparent to those skilled in the art upon reading this description in conjunction with the accompanying drawings, in which like reference numerals have been used to designate like elements, and in which:

[0017] FIG. 1 is a block diagram illustrating a basic model for providing content using DRM.

[0018] FIG. 2 is a block diagram illustrating a system for secure time management according to one aspect of the invention.

[0019] FIG. 3 is a flowchart illustrating a method of maintaining a secure date and time offset according to another aspect of the invention.

[0020] FIG. 4 is a flowchart illustrating a method of establishing an initial secure date and time offset according to another aspect of the invention.

[0021] FIG. 5 is a flowchart illustrating a method of evaluating DRM licenses having time-based usage rights according to another aspect of the invention.

DETAILED DESCRIPTION

[0022] To facilitate an understanding of exemplary embodiments, many aspects are described in terms of sequences of actions that can be performed by elements of a computer system. For example, it will be recognized that in each of the embodiments, the various actions can be performed by specialized circuits or circuitry (e.g., discrete logic gates interconnected to perform a specialized function), by program instructions being executed by one or more processors, or by a combination of both. Moreover, the exemplary embodiments can be considered part of any form of computer-readable

storage medium having an appropriate set of computer instructions that would cause a processor to carry out the techniques described here.

[0023] Thus, the invention can be embodied in many different forms, and all such forms are contemplated to be within the scope of what is claimed. Any such form of embodiment can be referred to herein as "logic configured to" perform a described action, or alternatively as "logic that" performs a described action.

[0024] FIG. 1 illustrates a basic model for providing content using DRM. A content provider 100 creates and packages digital content according to the DRM specification and establishes one or more sets of usage rights (or rules) and associated usage costs, which are associated with the various possible uses of the content (e.g., play, print, copy, distribute, etc.) and the allowable number of times, or time period, that the content is made available. The content is transferred to a distributor 110 that makes it available to users 120, for example on a distributor's storefront website. A user 120, operating user equipment (UE), may then browse the distributor's available content and select content of interest to the user 120, while also selecting one of the defined usage rights for the content (noting the associated usage costs). The user 120 makes the appropriate payment to the distributor 110 for the selected content/usage, at which time the content and usage rights can be transferred to the UE, which may be a mobile terminal or other device. The UE can then render the content according to the usage rules to make it available for use by the user 120 according to the usage rules. In some cases the rights are cleared through payment to an intermediary (not shown), such as a payment broker, which then signals the distributor 110 to supply the content.

[0025] The DRM-related data may be defined generally as two entities – a content container and a license – that can be transferred either as one physical package or as

two separate physical packages. The latter case is more flexible since a new license can be obtained without resending the entire content and a higher security level is achieved when content and license are not transferred together. If the content container and license are transferred separately, they each must include linking information.

[0026] The content container comprises the actual content that the user wants to render, which is typically in an encrypted form to protect against unauthorized usage. The license generally includes the usage rights of the associated content and some or all of the information needed to generate a key needed for content decryption.

[0027] As discussed above, the usage rights define the conditions that apply to the rendering of the content. To allow for flexible and extensible expression of the usage rights, special rights expression languages (REL) have been developed. Two of the dominating REL alternatives today are called extensible rights markup language (XrML) and open digital rights language (ODRL), both of which are based on extensible markup language (XML).

[0028] Platforms that support DRM-protected content distribution to the UE include some form of logical DRM component to provide the needed DRM functionality in the platform domain to process the DRM-protected content. For example, the platform for a telecommunications system must provide a logical DRM component to process the DRM-protected content that is made available for download to mobile terminals in the system. In general, the DRM component within the platform must provide DRM functionality support within the platform to an outside application (in the application domain) that is providing content to a UE supported by the platform.

[0029] The term platform as used here refers generally to platform software and hardware that at least partially make up a "secure" network in which users communicate, via UEs, either wirelessly or by wire, or any combination of the two. Network entities in the platform may be interfaced to outside applications in the application domain for the purposes of downloading DRM-protected content, among other things. The network is considered secure in the sense that the network platform and its communications traffic are managed and controlled by a network provider. As discussed above, there is added flexibility when the software is divided into a platform part, which is in the platform domain, and an application part, which is in the application domain. Any software requiring type-approval procedures, or other sensitive procedures, is preferably located in the platform domain.

[0030] An example of such a secure network is a telecommunications system, generally comprising UEs (e.g., mobile terminals) communicating wirelessly to base stations, which in turn communicate with other telecommunication network entities and the like. Included among these other entities is an interface to outside networks, such as the Internet, and outside applications. These outside applications are accessible to users within the network via the various network entities and the software they use to communicate and move data to and from the user (i.e., the platform software) under the control of the network provider.

[0031] FIG. 2 is a block diagram illustrating a system for secure time management according to one aspect of the invention. A platform 210 includes a DRM module 220 that manages the processing of DRM-protected content. The DRM module 220 parses license files, validates the usage rights associated with DRM-protected content, and performs other DRM-related procedures. Accordingly, the DRM module 220 also

validates time-based usage rights, i.e., DRM-protected content usage rights that set out prescribed time parameters, such as start and stop times or length-of-usage time. It is not necessary that the DRM module 220 be directly involved in the downloading of DRM-protected content or in the commercial transactions (e.g., browsing, payment, etc.) that may proceed downloading. Nevertheless, the DRM module may perform some or all of these functions as well.

[0032] The platform 210 also includes a clock server 230, a real-time clock (RTC) 250, and a secure time reference database (STRDB) 225. The clock server 230 exchanges time-related information with the DRM module 220 and RTC 250. The RTC 250 is a timing device associated with the UE (not shown) that enables the UE to keep track of time for time-based functions. In its simplest form, the RTC 250 comprises hardware and/or software that generate a series of periodic pulses, each pulse representing a unit of time, and the logic necessary to maintain a running time value based on the pulses and manage a proper time offset to represent the current time. The RTC 250 is typically housed in the UE, although this is not required. The "UE time value" can therefore be considered the RTC date and time value (RTCDT), which is typically used for many time-related functions of the UE and provides little or no security. That is, the RTCDT is accessible to a user of the UE, or other third parties, and can be changed through the use of an application (as discussed further below).

[0033] The vulnerability of the RTCDT to manipulation by a user or another party presents an opportunity for unauthorized use of DRM-protected content. For example, assume a user has purchased usage rights to play a particular group of audio files for a session of two hours at a start time of the user's choosing. The user begins the session at 1:00 PM, as determined by the RTCDT. The session is therefore scheduled to

expire at 3:00 PM. At 2:50 PM, however, the user changes the RTCDT back to 1:01 PM, for example. The user has just extended his session an additional unauthorized 1hr 49 min. The RTCDT, therefore, cannot be trusted.

[0034] According to this aspect of the invention, the DRM module 220 manages a secure time offset value (DRMSO) that is used to compensate for changes in the RTCDT. The DRMSO is then added to the RTCDT to obtain a secure date and time (DRMSDT), which is then available to the DRM module for time-based usage rights management. For instance, in the above example, when the RTCDT was changed by a value -1:49, a value +1:49 is added to the DRMSO to compensate. The DRMSDT, which is effectively the sum of the RTCDT and DRMSO, remains unchanged in the example so that the session expires after two hours as provided by the usage rights.

[0035] A DRMSO, and at least one other variable (discussed further below), is associated with each UE and is stored in the STRDB 225. As can be appreciated, the STRDB 225 can be an independent database, part of another database, or a component of the DRM module 220.

[0036] The clock server 230 has access to a secure time reference 235. For example, a network identity and time zone (NITZ) feature of a telecommunications system may be used to obtain a time reference value. In a telecommunication system, the NITZ provides enhanced roaming capabilities by providing the means for "serving networks" to transfer current identity, time, daylight-savings time, and local time zone information to mobile terminals. The NITZ is described in the 3rd Generation Partnership Project (3GPP) specification 3G TS 22.042, version 3.0.1.

[0037] It will, however, be understood that any secure time reference may be used, so long as the clock server 230 can communicate either directly or through intermediary

networks, network entities, and/or modules to obtain a reliable and secure time reference.

[0038] One or more applications 200, which are in the less secure application domain and are therefore suspect, may attempt to change the RTCDT. The application(s) may act in response to a time change request in the UE initiated by the user or a third party, or the application(s) 200 may initiate the time change themselves for any number of reasons.

[0039] According to an aspect of the invention, any application 200 attempting a time change in the RTC 240 communicates with the clock server 230. The clock server 230 then provides sufficient information about the time change to the DRM module 220 to update the associated DRMSO variable.

[0040] FIG. 3 is a flowchart illustrating a method of maintaining a secure DRMSO according to an aspect of the invention. When an application 200 attempts to change the RTCDT, the new value of the RTCDT is received by the clock server 230 (step 300). The clock server 230 retrieves the current RTCDT from the RTC 240 and determines the RTCDT difference, i.e., the current RTCDT subtracted from the new RTCDT (step 310). The RTCDT difference is provided to the DRM module 220 (step 320). The DRM module 220 then adjusts the associated DRMSO in the STRDB 225 to compensate for the time change (step 330).

[0041] For example, if the application 200 sets the time back three hours, the RTCDT difference = -3 hrs. The DRM module 220 adjusts the associated DRMSO to +3 hrs to compensate. When a DRM license is received for evaluation by the DRM module 220, the DRMSDT (= RTCDT + DRMSO) calculated by the DRM module to evaluate the usage rights is unaffected by the RTCDT difference.

[0042] The method described above in FIG. 3 presupposes that the DRMSO is initially correct. More particularly, the method of FIG. 3 presupposes that the DRMSO has been previously set to an offset value that, when added to the RTCDT, the resulting DRMSDT value represents the current secure date and time. Subsequent adjustments to the DRMSO are then performed as described in method of FIG. 3.

[0043] The DRMSO must therefore be set initially according to a trustworthy, i.e., secure, time reference, since the RTCDT is not secure. In addition, the RTC 240 may be reset, or first initialized, which would provide an RTCDT value that is not referenced to the current time, i.e., the RTCDT's relation to the current time is indeterminate. In each of these cases, the DRMSO must be initially set, or reset, to a value that is based on a secure time reference 235, such as the NITZ, as mentioned above.

[0044] The DRM module 220 also maintains, in the STRDB 225, a DRM secure clock state (DRMSCS) variable that is associated with each UE. In its simplest form, there are two possible values for DRMSCS, "secure" and "not secure". The DRMSCS indicates whether or not the DRMSO is considered to be a secure value. In general, the DRMSCS for each terminal is initialized to "not secure" until the DRMSO is at least initially referenced to a secure time reference. In general, the DRMSCS may be considered an indication as to whether the DRMSO should be updated, i.e., an "update indicator".

[0045] FIG. 4 is a flowchart illustrating a method for establishing an initial secure DRMSO according to another aspect of the invention. First, it is determined whether the DRMSCS associated with a UE is already set to "secure" (step 400), and if not the clock server 230 retrieves the current date and time from the secure time reference 235 (step 410).

[0046] Alternatively, the clock server 230 may already be aware of the current date and time, in which case step 410 may be omitted. For example, the clock server 230 may maintain the current date and time and periodically, e.g., once every minute, hour, or day, synchronize to the secure time reference 235.

[0047] It is determined whether an RTC 240 associated with the UE is properly initialized (step 415). Even after an initialization, an RTC 240 can become "uninitialized" for a variety of reasons. For example, if the RTC 240 is reset or the battery is removed for an extended period of time, the RTC 240 becomes unitialized. The RTC 240 includes logic to indicate the unitialized state to the DRM module 220, e.g., via the clock server 230, once power and communication ability is restored to the RTC 240.

[0048] If the RTC is properly initialized, then the clock server 230 reads the current RTCDT from the RTC 240 and determines the difference between the time reference and the RTCDT, i.e., the current RTCDT subtracted from the time reference (step 420). The time difference is provided to the DRM module 220 (step 430). The DRM module 220 then sets the associated DRMSO in the STRDB 225 to the received time difference value (step 440). The DRMSO is first considered secure after setting the DRMSO according to the secure time reference 235, as described above, at which time the DRMSCS is set to "secure" to indicate a secure DRMSO (step 450).

[0049] For example, if the time difference = -3 hrs. The DRM module 220 sets the associated DRMSO to the same value, -3 hrs. When a DRM license is received for evaluation by the DRM module 220, a correct DRMSDT (= RTCDT + DRMSO) that corresponds to the secure time reference is calculated by the DRM module to evaluate the usage rights.

[0050] If, however, the RTC is not properly initialized (step 415), the RTC value is set to the value of the retrieved time reference (step 460). A time difference of zero is provided to the DRM module 220 (step 470). The DRM module 220 then sets the associated DRMSO in the STRDB 225 to the received time difference value, which is zero in this case (step 440). The DRMSO is first considered secure after setting the DRMSO according to the secure time reference 235, as described above, at which time the DRMSCS is set to "secure" to indicate a secure DRMSO (step 450).

[0051] FIG. 5 is a flowchart illustrating a method of evaluating DRM licenses having time-based usage rights according to yet another aspect of the invention. When the DRM module 220 receives a license validation request for time-based usage rights (step 500), the DRM module 220 determines if the DRMSCS associated with the respective UE has a value of "secure" (step 510). If the DRMSCS = "not secure", the license is considered invalid by the DRM module 220 and the content is not made available to the UE (step 540). Alternatively, if the DRMSCS = "secure", the license is evaluated by the DRM module 220 to determine the time parameters of the time-based usage rights (step 520), and if the time parameters cover the current DRMSDT (= DRMSO + RTCDT), the content is rendered and made available to the UE for use according to the usage rights (step 530). A rendering server (not shown) may be employed to render the content.

[0052] It will be appreciated by those of ordinary skill in the art that the invention can be embodied in various specific forms without departing from its essential characteristics. The disclosed embodiments are considered in all respects to be illustrative and not restrictive. The scope of the invention is indicated by the appended

claims, rather than the foregoing description, and all changes that come within the meaning and range of equivalents thereof are intended to be embraced thereby.